RFID

A Radio Frequency Identifiers (RFID) card transmits bits over radio. It uses electromagentic field to communicate. Some tags are passive, which means that they are activated by the reader. Some tags are active and does therefore require a local powersource (like a battery). The higher the frequency the more bits can be sent per second.

RFID always implied the following: - a tag - a reader - an antenna

NFC

NFC - Near Field Communication is a set of protocols. These protocols allows to devices to exchange information within 4 centimeters. They operate on the same range as RFID. The main purpose of NFC was to allow both the tag and the reader to send and recieve information. With RFID a tag can only send information, but not receive it.

Trademarks

There are many known trademarks. Producers of chips that use RFID technology.

Some common ones are EM, HID and MIFARE

MIFARE

MIFARE is a trademark for a series of chips. MIFARE is owned by NXP semiconductors which was previously Philips Electronics. So it is just a chip, which uses RFID technology.

MIFARE is split into four main groups.

1. MIFARE Classic 1k/4k. It can store 1025 bytes or 4096 bytes. The memory/disk is divided into different sectors and blocks. It is used for access badges.
2. MIFARE ultralight - A 64 byte version fo MIFARE Classic. Is cheap to make. So it is used for disposable ticketsfor events and transportation.
3. MIFARE Plus - The replacement for Classic. With 128-bit AES encryption.
4. MIFARE DESFire - Comes with the OS DESFire, which contains a filestructure and files. The best in terms of security.

Identify your card

You place the card on the reader and run `lf search`.

If it responds like this:

```
EM410x pattern found:
```

You have found a tag with EM410x. It runs on 125 kHz. It is a low frequency chip.

You will probably see something like this:

```
EM410x pattern found:

EM TAG ID      : 00002A3B26
```

If you have gotten the TAG ID, you can choose to either Emulate it, which tells Proxmark to act like that tag. It will then send out the same pattern as the card itself, and you can get into the door. Or you can simply clone it.

With this knowledge you can now use more specific EM410 commands.

```
lf help

[...]
em              { EM4X CHIPs & RFIDs...      }
[...]
```

```
proxmark3> lf em
help            This help
410xread        [findone] -- Extract ID from EM410x tag (option 0 for continuous loop, 1 for only 1 tag)
410xdemod       [clock] [invert<0|1>] [maxErr] -- Demodulate an EM410x tag from GraphBuffer (args optional)
410xsim         <UID> [clock rate] -- Simulate EM410x tag
410xbrute       ids.txt [d (delay in ms)] [c (clock rate)] -- Reader bruteforce attack by simulating EM410x tags
410xwatch       ['h'] -- Watches for EM410x 125/134 kHz tags (option 'h' for 134)
410xspoof       ['h'] --- Watches for EM410x 125/134 kHz tags, and replays them. (option 'h' for 134)
410xwrite       <UID> <'0' T5555> <'1' T55x7> [clock rate] -- Write EM410x UID to T5555(Q5) or T55x7 tag, optionally setting clock
```

Clone the EM410

You need to first read the data of the tag, and then write it somewhere. You can use a T55x7 tag to write it to. I got a T5577 with my proxmark. So just put your T5577 tag on your proxmark, and then run the following command:

You take the TAG ID, that was previously identified and you run it like this:

```
proxmark3> lf em4x em410xwrite 00002A3B26 1
```

Now it should have been written to your tag, and it should work.